May 27, 2016

**Filed electronically**

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

**Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106**

Dear Ms. Dortch:

I respectfully submit the attached Supplemental Comment for the above-referenced matter. Please let me know if you have any questions.

Sincerely,

Shawn Sheridan
Turlock, California

Attachment

cc (via email):

| | | |
|---|---|---|
| Amy Bender | Daniel Kahn | Edward Smith |
| David Brody | Melissa Kirkel | Gigi Sohn |
| Brendan Carr | Travis Litman | Jennifer Tatel |
| Robin Colwell | Charles Matthias | Johanna Thomas |
| Matt DelNero | Erin McGrath | Stephanie Weiner |
| Rebekah Goodheart | Bakari Middleton | Jon Wilkins |
| Lisa Hone | Ruth Milkman | Sherry Wood |
| Scott Jordan | Sherwin Siy | |

**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Protecting the Privacy of Customers of Broadband and Other Telecommunications Services | ) | WC Docket No. 16-106 |
| | ) | |

## SUPPLEMENTAL COMMENT

Filed: **May 27, 2016**

By: Shawn Sheridan
290 N. Thor St., Apt. 200
Turlock, CA 95380-4000
sheridan3398@yahoo.com

## TABLE OF CONTENTS

## I. DECLARATION

1. I declare under penalty of perjury under the laws of the State of California that the following is true and correct:

> My authorship of and personal experiences expressed in this Supplemental Comment for WC Docket 16-106, as well as filings at fcc.gov for MB Docket 15-149.[1]
>
> Clarification: I am a former subscriber to video, voice *and* Internet services, separately.[2]

Date executed: May 27, 2016
Place: Turlock, California; County of Stanislaus
Signature: */s/ Shawn D. Sheridan*
Shawn D. Sheridan

## II. INTRODUCTION

2. There are very few American citizens who can say that a Comment submitted to the Federal Communications Commission prompted a military response. That is what occurred on Thursday, May 19, 2016. The day after filing my Comment online for WC Docket 16-106,[3] a gray C-130 size military aircraft flew less than 1000 feet above my local library as I was walking toward it to access the Internet using my Wi-Fi only iPad.

3. I live four blocks away, but I was two blocks away when the plane flew over. The sky was still bright. Then, while standing outside of the library and connected to the free Wi-Fi, at 6:40 p.m. the same plane flew over from the same direction as before, practically above the trees. I decided to walk to FedEx Office less than a mile away to see if I could get the plane to fly over there, as well, but when I was four blocks away (not in the direction of my residence) I watched the same plane fly above the library a third time.[4] I then looked up and saw a gray 737 size plane flying at a higher altitude.

4. Upon arriving at FedEx Office, I accessed the free Wi-Fi using my iPad for a few minutes, then walked across the street waiting to take a photo. By then the sun was beginning to set, but the C-130 flew near my location at a higher altitude and sharply turned so that the belly of the plane faced FedEx Office. At the same time a 737 type plane flew overhead, but too high to photograph with my iPad. Both planes then left Turlock at the same time and direction (west).

---

[1] In the Matter of Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership for Consent to Transfer Control of Licenses and Authorizations. *See* Oct. 17, 2015 Letter; Nov. 12, 2015 Reply to Responses/Oppositions at 31; Dec. 27, 2015 Supplemental Reply to Responses/Oppositions at 23; Jan. 19, 2016 Additional Reply to Responses/Oppositions at 12; Feb. 4, 2016 Letter; April 11, 17 and 27, 2016 Letters for MB Docket 15-149.

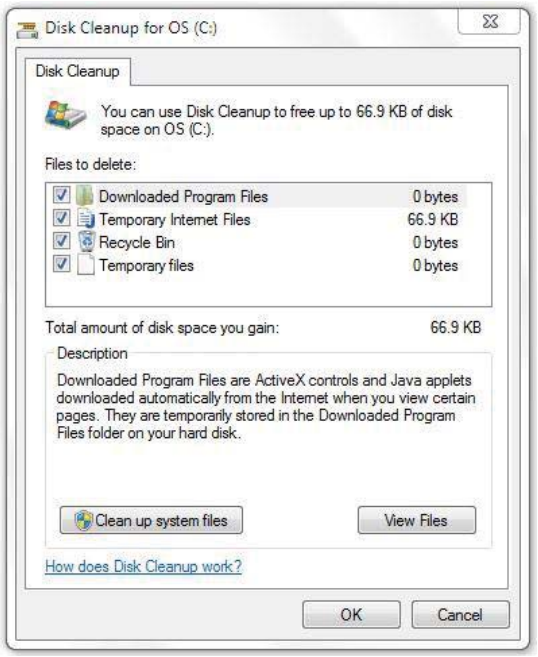
[2] In my previous Comment, I stated: "I am a former subscriber to video, voice, or Internet service."

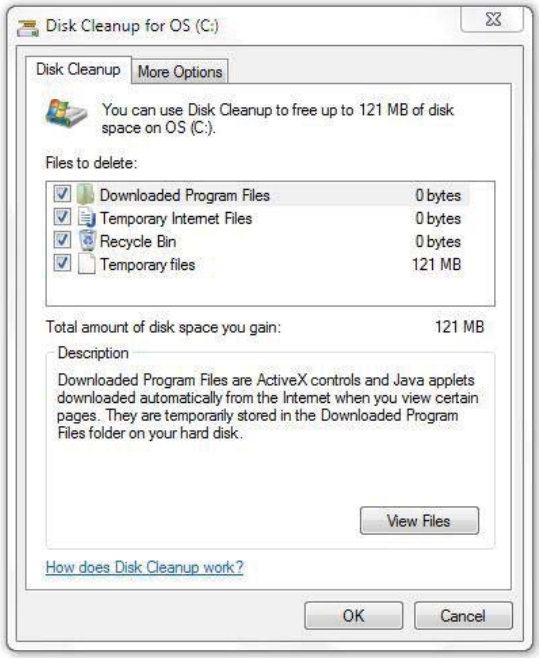
[3] Filed on May 18, 2016 at fcc.gov.

[4] Three extremely low flyovers of a C-130 type plane were so surprising that I didn't make a photo with my iPad.

5. On Friday, May 20, my mother, sister, nephew and I were standing outside my sister's house in the cul-de-sac at 3:30 p.m., when the very familiar blue-and-white twin-engine plane flew over us exceedingly fast less than five hundred feet (500 ft) in altitude. At 7:45 p.m. I was outside of my residence when I witnessed a 737 type plane fly in an S formation overhead. At 8:30 p.m. a dark-colored 737 type plane flew slowly over my residence. These incidents are among many, many flyovers by smaller planes (*see* X. Exhibits).

6. On Tuesday, May 24, 2016 I decided to begin typing this new Comment with my laptop that had not been turned on for several days. Within minutes of turning my laptop on, two planes flew over and several files were inserted without being connected to the Internet. As mentioned in my prior Comment,[5] I have not accessed the Internet at my current residence even once. The first image below was made at 11:30 a.m. when files began appearing. The second image, of 121 MB of temporary files, was made at 11:35 *p*.m. after my laptop had been in sleep mode for several hours with most system settings disabled—not connected to the Internet.[6]




7. On Wednesday, May 25, I was sitting outside of the library accessing the Internet with my iPad when I heard two planes approach. Generally I've turned off Wi-Fi and locked the screen until planes can no longer be heard, but on that day I decided to continue with what I was doing: saving a PDF to Apple's iBooks app of the Communications Act of 1934. As one of the planes flew directly overhead, my "Save PDF to iBooks" feature in the Safari web browser app suddenly disappeared, as well as the ability to save a PDF to my Adobe Acrobat app. No matter what website I went to, those features were no longer available. I closed and re-opened Safari, but no change. It wasn't until I re-started the device that the features re-appeared.

[5] Footnote 5 at page 4, filed on May 18, 2016 for WC Docket 16-106.

[6] The second image was derived after clicking the "Clean up system files" button. This is why I have to turn my Dell laptop off and remove the battery when not in use.

8. On the same day I did something I hadn't done, which was use a flash drive on a public library non-wireless computer. I inserted the flash drive and initially used the Chrome web browser for generic searches that could not pinpoint to me. I decided to test if the library's computers were indeed under surveillance, so I deliberately searched via Google.com for "In-Q-Tel". Within two minutes, the screen flickered and became slightly blurry, then went back to normal. My flash drive was connected to the computer at the time. When I went home I plugged the flash drive into my Dell laptop and noticed that a file had been inserted on the drive with a Google Chrome icon. The name of the file: Traces. As soon as I clicked for the Kaspersky anti-virus software to scan the drive, from that point until now, when my Kaspersky application is open, the screen is completely white. Even though the application seems to operate, I neither can access the interface on my laptop screen nor close the application once it has been opened (it now only closes after restarting the laptop).

9. On Thursday, May 26, at 3:15 p.m., the following is what I saw while standing one block from the library:

10. One American citizen, who filed comments at fcc.gov about things concerning the Charter/Time Warner merger, as well as privacy protections, has garnered expensive attention. I wish I knew the names of those who authorized operations against me, but who can know?

11. In this Introduction, I present one more photo to the Commission of the types of aircraft that have flown over my locations. The following was made on May 25, 2016:

12. Due to the Commission's Notice of Proposed Rulemaking (NPRM or Notice) involving hundreds of considerations to which comments are sought, I present this Supplemental Comment—despite being under pervasive, unethical surveillance.

## III. UNDENIABILITY OF MASS MONITORING

13. There is significant difference between providing customers of broadband Internet access service (BIAS) with controlling tools and protecting customers from accesses, as well as lawful uses and misuses, of customer proprietary network information (CPNI).

14. My previous Comment established that it is impossible for subscribers of BIAS to protect against perpetual intrusions from unmentionable third parties via government-sponsored monitoring and surveillance.[7] The most powerful tool that can be imposed upon BIAS providers could only protect against non-government-authorized misuse of CPNI. No customer tool can protect against **government-authorized access and misuse**, because authorized private-sector third parties can misuse CPNI without accountability.

15. As the Commission proceeds, there should be an inclusive understanding that the age of big data analytics is not evolutionary, but rather incited by U.S. federal law and funding. Unprecedented mass monitoring, mass data collection, storage and analysis, mass profiling, etc., now passes through an unknown amount of U.S. and foreign technology companies.

16. Something I missed in my previous Comment was found in a publically-available downloaded PDF. The title: "Electronic Surveillance Manual, Procedures and Case Law, Forms (Revised June 2005)".[8] Regarding the Communications Assistance for Law Enforcement Act (CALEA), the manual states on page 48:

> "C. The Inapplicability of CALEA's Prohibition on Collection Using Pen/Trap Authority
>
> In passing CALEA in 1994, Congress required providers to isolate and provide to the government certain information relating to telephone communications. At the same time that it created these obligations, it created an exception: carriers shall not provide law enforcement with "any information that may disclose the physical location of the subscriber" in response to a pen/trap order. (A fuller quotation of the language appears, above, in Section I.B.). By its very terms, this prohibition applies only to information collected by a provider and not to information collected directly by law enforcement authorities. Thus, CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate targeted cell phones."

17. One aspect of the quoted text is that it mentioned "law enforcement authorities" instead of "pursuant to a court order or other lawful authorization" mentioned in the CALEA.[9] Like Microsoft, mentioned in my prior Comment as utilizing "independent civil authorities,"[10] it can be said that authorities used to handle CPNI broadly span corporate and government levels.

18. Due specifically to lawful authorizations of mass monitoring, as well as targeted surveillances conducted by unknown actors, BIAS privacy protections are grossly limited. The CALEA's definition of government includes "any agency *or instrumentality thereof*...authorized by law to conduct electronic surveillance."[11] Again, there are hundreds of authorized private-sector third parties allowed to access CPNI—whole or in part—with or without customer choice. At minimum, the Commission should mandate privacy notices that inform customers of realities of directly unavoidable exposures to third parties.

---

[7] Paras. 15-58 of Comment filed on May 18, 2016 for WC Docket 16-106.

[8] I do not have or remember the Internet source of the PDF. The Introduction partly states: "This manual sets forth the procedures established by the Criminal Division of the Department of Justice to obtain authorization to conduct electronic surveillance pursuant to Title 18, United States Code, Sections 2510-2522 (2001) (Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 (ECPA), the Communications Assistance for Law Enforcement Act of 1994 (CALEA), the Antiterrorism and Effective Death Penalty Act of 1996 (Antiterrorism Act)), the USA-Patriot Act of 2001, and the Homeland Security Act of 2002 and discusses the statutory requirements of each of the pleadings. Throughout this manual, the above federal wiretap statutes will occasionally be referred to collectively as "Title III."

[9] CALEA, Sec. 103(a)(1).

[10] Para. 27 of Comment filed on May 18, 2016 for WC Docket 16-106.

[11] CALEA, Sec. 102(5).

19. Notifying customers of lawful monitoring is not a national security matter which could cause the masses to go into hiding, but rather informing common consumers of the lack of privacy afforded if using electronic services. When someone goes to a public swimming pool, a sign is not posted to read: "The lifeguards are required to keep you safe." It generally reads: "Swim at your own risk." For purposes of this Comment, I urge the Commission to acknowledge realities of today by mandating notification to unassuming and uninformed customers about what is lawfully relinquished by using electronic services.

20. Also, paragraph 307 of the *Notice* states: "We believe that Section 705 [of the Communications Act of 1934] can thus provide a source of authority for rules protecting the privacy of customer information, including the content of their communications. Do commenters agree?" I do not agree, because Congress usurped Section 705(e)—fines and/or imprisonment for willful violations—with laws that mandate both access to CPNI and secrecy by unaccountable third parties.

21. Section 705(a) involves interceptions of communications, so Section 705(e)(1) is practically unenforceable in instances such as a rogue employee of a government-authorized third party secretly mishandling CPNI. Microsoft's Cybercrime Center is an example of secret, not-to-be-made-public operations,[12] so how would violations made there be known by victims? If containable, Microsoft would not make public a rogue employee's act(s), but rather address the employee and go about their secret operations.

22. It is documented in my comments and letters for MB Docket 15-149 regarding Charter Communications (Charter) that I initiated a billing dispute in April 2014, that remains entirely unresolved two years later. The Commission is aware of the matter that escalated to the board of directors, and the prime tactic Charter has used has been to ignore me. Today, what can the Commission do about that? Could I trust the Commission to step in if Charter was/is guilty of improperly disclosing my CPNI? It's difficult to expose violators when collusion is cultural.

23. With Charter now a powerful corporation, what makes the Commission think that a provider such as Charter would notify a customer of misuse of CPNI when it was done by the provider? If a BIAS provider willfully misuses CPNI without the customer knowledge, why would notice be sent to the one violated? It's called collusion. That's why it's been difficult to understand the reason(s) for the Commission's concern to update privacy protections specifically for BIAS providers, because the gatekeeper knows who and when to inform and not inform to remain safe from any harm.

## IV. GEO-LOCATION

24. Paragraph 4 of the *Notice* states: "And [BIAS providers] have control of a great deal of data that must be protected against data breaches." The paragraph describes some of that data as the customer's location. Since Apple and Samsung are customers of Skyhook Wireless,[13] the company that provides geo-location for their devices, how can a BIAS provider safeguard information utilized by third-party Skyhook Wireless that is both constant and instantaneous? Newly-bought devices must be initially setup, and Skyhook Wireless is able to obtain the device ID and location information with the first connection to the Internet.

25. In paragraph 12 of the *Notice*, the Commission used the example of Weather.com seeking express consent before collecting geo-location. That type of consent does not prohibit knowing a visitor's general location, but rather impacts the viewing preference.

26. YouTube is a similar example. If I go to YouTube.com without signing in, such as when using a public computer at a local library, the home page provides generic selections of videos. But if I sign in, the home page will change based on my personal viewing history, and only if I haven't disabled the setting for YouTube to maintain that history. Weather.com provides both generic and location-based experiences as part of its features, which is not comparable to a BIAS provider being able to prohibit or safeguard device locations at all times.

27. If BIAS providers gave customers a choice not to be located by their devices, it would be impossible to keep third parties from knowing a customer's location, with or without that choice. This is partly a tragedy, because my location should be private if I so choose, but it is made known by force when accessing the Internet via an identifiable or identified device due to companies like TruePosition[14] and Skyhook Wireless.

28. Skyhook Wireless' website states that it uses technology that can locate a device within 20 meters. How hard would it be to identify an individual's address if the location of a tablet or smartphone consistently remained at night at only one house? How hard would it be to identify a person's vehicle as soon as a phone call was made through the vehicle's technology? How hard would it be to identify a person's place of work when the device is often located there?

29. There is a difference between ability to locate a device with or without consent and having settings to not provide particular services or features dependent upon geo-location. The Commission rightfully seeks to define geo-location as personal information, but should acknowledge that it is not safeguarded against laws that mandate access to CPNI by third parties who simultaneously serve private sector customers and the government. However, though many considerations were presented in the *Notice*, § 64.7000(g) of Appendix A—Proposed Rules—does not seem to alter the definition of CPNI at all.

## V. AGGREGATE CUSTOMER INFORMATION

30. Paragraph 156 of the *Notice* states: "To the greatest extent possible, we ask that commenters ground their comments in practical examples: what kinds of aggregate, non-identifiable information do or can BIAS providers use and share?" That is an interesting question since Section 222(h)(2) of the Communications Act specifically used the words *group*, *category*, *services*, *customers*, *identities*, and *characteristics*; and Section 222(c)(3) specifically used the word *nondiscriminatory*.

(Continued from previous page) ———————————————

[12] *See* article, *Digital Detectives*, at http://news.microsoft.com/stories/cybercrimes/index.html (Nov. 2013).

[13] The website, www.skyhookwireless.com, states: "Skyhook's massive global network powers billions of location requests in all of the places that they happen. Our customers include giants like Apple, Samsung...."

[14] *See* http://www.trueposition.com *and* http://www.trueposition.com/products/truefix-platform.

| | | |
|---|---|---|
| group of services | = | applicable to voice, video and Internet services |
| group of customers | = | applicable to voice, video and Internet services |
| category of services | = | applicable to voice, video and Internet services |
| category of customers | = | applicable to voice, video and Internet services |

31. In context, voice service is not different than Internet service with a device that both makes phone calls and sends emails. Also in context, the aggregate customer information specifically applies to telecommunications carriers.

32. The aspect of Section 222(h)(2) that not even a characteristic of an individual customer can be involved begs the question, what type of information can be linked to customers but not linked to individual customers? Commenters can guess, and savvy commenters can give good examples, but since the Communications Act has been in force since 1934, such a question could best be answered by telecommunications carriers and BIAS providers.

33. Statistical data, monitoring of traffic in a certain area and equipment load would probably be on the list, but even statistical data may contain characteristics. For example, when I view statistical data for a video I uploaded at YouTube, I'm informed of which state and country the viewers were located, whether someone viewed the video after clicking on a third party link, male viewers versus female, etc.

34. In my opinion, if aggregate data contains locations of customers and/or devices more specific than postal (zip) codes, that data would contain characteristics of individual users. As to other words involved, such as "nondiscriminatory" in Section 222(c)(3), it suggests that as information is gathered, both identities and characteristics are initially part of the collection and then removed. How could that word be more than guidance for those assembling the information, because who outside could know if discrimination occurred unless it was conspicuous?

35. The Commission suggests in paragraph 158 of the *Notice* to provide guidance to BIAS providers of what is meant by linked and linkable information. I urge the Commission, if possible, to not provide that as guidance, but rather requirement that linkable information should be treated the same as linked information.

## VI. DEFINING BIAS PROVIDER

36. The *Notice* presents ISPs as 'BIAS provider' instead of 'provider of BIAS' which is fundamentally different in the context of the proposed rules. Legacy AT&T, for example, did not begin as a BIAS provider, but both now provides BIAS. Charter, for example, provides voice, video and Internet services to the same residential customer. If the Commission intends to define a BIAS provider as a separate entity from a telecommunications carrier, it will not reflect the major providers of today.

## VII. THE FUTURE OF BIAS

### A. Mobile Virtual Network Operator

37. An article by Multichannel.com, *Technology: The Straw That Stirs Cable's Drink*, quotes Liberty Global's executive vice president and chief technology officer, Balan Nair—also a director of Charter Communications—who described the push for the mobile virtual network operator (MVNO) model and also "WiFi-first" devices.[15] That article describes how LTE phones will be designed to connect to nearby Wi-Fi before using cellular signals, which of course, will pinpoint an individual even more and also involve BIAS far more, any time, anywhere.

### B. Dark Fiber

38. An article by Wired.com, Facebook And Microsoft Are Laying A Giant Cable Across The Atlantic, describes how they are building their own networking infrastructure both on land and across the seas.[16] The article mentions the use of "dark fiber" referring to "The Real Telecoms."

### C. Stratobus

39. A recent press release from a French company described a new project in which pseudo satellites will be placed in the stratosphere that can remain in place for a long period and monitor telecommunications, etc., as well as conduct surveillances.[17]

40. For such a critical matter as the Commission's *Notice* involves, it would be a true disservice to Americans if the matter remained neglectful of government-sponsored monitoring and providers of other services and providers that also pertain to the same type of CPNI.

[continued on next page]

[15] http://www.multichannel.com/news/cable-tv-conventions/technology-straw-stirs-cable-s-drink/394635; published October 19, 2015.

[16] http://www.wired.com/2016/05/facebook-microsoft-laying-giant-cable-across-atlantic/; published May 26, 2016.

[17] https://www.thalesgroup.com/en/worldwide/space/press-release/stratobus-project-takes; published April 26, 2016.

## VIII. EXHIBITS

41. The following are photos that have not been presented to the Commission, and are for the purpose of providing additional proof of what I have been conveying regarding various airplanes and helicopters daily flying over my locations since at least October 2015.

42. This photo—made on May 25—is of a plane that has flown over me countless times at my residence, the library, my sister's house, etc. On May 26, while standing outside at my sister's house, this plane flew slowly at perhaps 500 feet altitude directly over her house.

43. This photo—made on May 24—is of the very familiar blue-and-white twin engine plane that I haven't been able to get a close-up. After seven months of surveillance, only recently have I taken time to make photos, specifically for my comments to the Commission.

44. This photo—made on May 22—is of a plane that has flown over my locations many, many times. These planes seem to depart from the Modesto City-County Airport, located about 10 miles away, and other times from the Turlock Municipal Airport, located about 10 miles away in the opposite direction.

45. This photo—made on May 14—is of a plane that looks like an old crop duster. However, it most certainly has been used to fly over my locations. On May 25, 2016 I heard a plane approaching as I was typing this document. It sounded very low, but I didn't take the time to get a camera and go outside. This plane flew so low overhead that I rushed outside without a camera and the plane looked to be only hundreds of feet in altitude, practically above the trees.